DE LA «LIBERTAD INFORMÁTICA» A LA CONSTITUCIONALIZACIÓN DE NUEVOS DERECHOS DIGITALES (1978-2018)

ARTEMI RALLO LOMBARTE

SUMARIO

Fecha recepción: 28.06.2017
Fecha aceptación: 3.10.2017

DE LA «LIBERTAD INFORMÁTICA» A LA CONSTITUCIONALIZACIÓN DE NUEVOS DERECHOS DIGITALES (1978-2018)[1]

ARTEMI RALLO LOMBARTE[2]

Catedrático Derecho Constitucional
Universidad Jaume I de Castellón

I. INTRODUCCIÓN

La sociedad española ha protagonizado transformaciones extraordinarias a lo largo de las últimas cuatro décadas[3]. Los cambios sociales, económicos, institucionales o culturales han resultado sobresalientes. España se incorporó a las sociedades democráticas avanzadas que disfrutan de los mayores avances económicos y sociales y de un sistema de garantía de los derechos fundamentales de irreprochable verificación práctica.

Pero los principales cambios sociales operados en la sociedad española durante los últimos cuarenta años no tienen una dimensión nacional si no global:

[1] Este trabajo ha sido elaborado en el marco del proyecto de investigación financiado por el Ministerio de Economía y Competitividad (DER2015-63635-R) sobre «El impacto del nuevo Reglamento Europeo de Protección de Datos: análisis nacional y comparado» del que el autor fue, inicialmente, investigador principal. Una primera versión será publicada en 2018 en la obra colectiva editada por el Centro de Estudios Políticos y Constitucionales conmemorativa del 40 Aniversario de la aprobación de la Constitución España de 1978.

[2] Catedrático de Derecho Constitucional. Departamento de Derecho Público. Facultad de Ciencias Jurídicas y Económicas. Universitat Jaume I. Avda. de Vicent Sos Baynat, s/n. E-12071 Castelló de la Plana. España (Spain). Email: rallo@dpu.uji.es

[3] Pérez Luño, A. E. (2012): *Los derechos humanos en la sociedad tecnológica,* Universitas, Madrid; Díaz Revorio, F. J. (2009): *Los Derechos Humanos ante los nuevos avances Científicos y Tecnológicos: Genética e Internet ante la Constitución*, Tirant lo Blanch, Valencia.

durante este periodo de tiempo el mundo ha conocido una revolución tecnológica, imposible de predecir medio siglo atrás, que ha modificado sustancialmente las pautas de comportamiento y relaciones humanas[4]. Lo que implica la existencia de una sociedad distinta en la que el ser humano se relaciona de forma diferente y en la que numerosas categorías inherentes a la existencia humana han mutado en un escenario diferente. La tecnología está cambiando nuestra sociedad para hacernos mejores y ofrecernos más y mejor vida: más cultura, más información, más libertad, más democracia, etc.[5].

Obviamente, el Derecho, como ciencia social llamada a regular y ordenar los comportamientos humanos, no ha resultado inmune a las transformaciones sociales causadas por la revolución tecnológica y ha sufrido las modificaciones inevitables y necesarias para someter las nuevas conductas vinculadas al cambio tecnológico.

La meritoria —por expresa y vanguardista— referencia a *la informática* en el texto constitucional de 1978 constituyó un innegable aldabonazo para otorgar trascendencia constitucional a la necesaria protección del individuo frente a los riesgos que sobre él —y, particularmente, sobre el disfrute de algunos de sus derechos fundamentales— cernían los avances tecnológicos ligados a la incipiente y primaria computerización [6].

Cuatro décadas después —viviendo en plena sociedad de la información y del conocimiento, culminando con toda intensidad la era digital y apenas adentrándonos en los terrenos inexplorados e inciertos de la inteligencia artificial—, resulta incuestionable que la sociedad contemporánea afronta el reto mayúsculo de constitucionalizar nuevos derechos que satisfagan la demanda social de protección frente a riesgos y amenazas presentes y futuras [7].

En este espacio de tiempo —relativamente breve si lo relacionamos con la magnitud de los cambios sociales producidos— los poderes públicos no han permanecido ajenos a las necesarias modificaciones normativas que debían acompañar los cambios tecnológicos. En España, sendas leyes (LORTAD y LOPD) — a las que en un futuro inmediato se unirá la Ley Orgánica de Adaptación de la LOPD al Reglamento General de Protección de Datos— son reconocidas con

---

[4] Castells, M. (2011): *La galaxia Internet*, Areté, Barcelona.

[5] Rovira, A. (1992): «Reflexiones sobre el derecho a la intimidad en relación con la informática, la medicina y los medios de comunicación», *Revista de Estudios Políticos*, núm. 77, pp. 259 a 265.

[6] Lucas Murillo de la Cueva, P. (1990): *El derecho a la autodeterminación informativa*, Tecnos.

[7] Troncoso Reigada, A. (2010): *La protección de datos personales en busca del equilibrio*, Tirant lo Blanch, Valencia.

el honroso título de normas de desarrollo del precepto constitucional que consagra la garantía de los derechos frente al uso de la informática. Tal reconocimiento resulta notablemente deudor de la hermenéutica constitucional que, del mandato constitucional dirigido a los poderes públicos para preservar a los individuos frente a los riesgos y amenazas de la tecnología, dedujo con valentía y determinación un derecho fundamental autónomo —denominado, inicialmente y con singular originalidad, *libertad informática* y, posteriormente, en forma más prosaica, derecho a la protección de datos— de efectos expansivos extraordinarios. Jurisprudencia constitucional —y, en numerosas ocasiones, ordinaria— que ha tenido durante las últimas décadas notables dificultades para otorgar plenitud dogmática al derecho a la protección de datos obligándolo a convivir simbióticamente con el ya consolidado y homologado dogmáticamente derecho a la intimidad/privacidad.

Sin embargo, pudiera parecer de lo anteriormente apuntado que es mérito exclusivamente patrio la respuesta constituyente o legislativa a la necesidad de garantizar derechos fundamentales frente al cambio tecnológico: nada más lejos de la realidad.

La propia constitucionalización del *fenómeno informático* en sede de garantía de derechos fundamentales, como veremos, no es ajena a un contexto comparado de atención ineludible a finales de la década de los setenta.

Pero más relevante aún resulta constatar que los desarrollos legislativos conocidos en nuestro país en 1992 y 1999 —también el de inminente aprobación en 2018— no constituyen tanto iniciativa propia nacional como el inevitable resultado de la obligación de cumplir con los compromisos internacionales adquiridos por España en el orden internacional (al ratificar el Convenio 108 del Consejo de Europa de 1981) y europeo (al trasponer la Directiva 95/46, consagrarse el artículo 8 de la CDFUE [8] o adoptarse el Reglamento UE 2016/679).

La reciente aprobación (2016) e inminente entrada en vigor del Reglamento Europeo de Protección de Datos (2018) —aunque resulte acompañada de una casi prescindible legislación nacional de adaptación del mismo—, de directa aplicación en todos los Estados miembros, evidencia la irreversible *europeización* de la estrategia pública de protección de los derechos fundamentales frente a la tecnología que ya fue iniciada por la Directiva 95/46, que el artículo 8 CDFUE [9] ya consagró al

[8] Guerrero Pico, M. C. (2005): «El derecho fundamental a la protección de los datos de carácter personal en la Constitución Europea», *Revista de Derecho Constitucional Europeo*, núm. 4, pp. 293 a 334.

[9] Ruiz Miguel, C. (2003): «El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico», *Revista de Derecho Comunitario Europeo*, núm. 14, pp. 7 a 43.

elevar a rango constitucional europeo un derecho fundamental autónomo a la protección de datos y que la jurisprudencia europea (singularmente, del TJUE) ha contribuido a consolidar inequívocamente en sucesivos pronunciamientos que han configurado una jurisdicción garante de los derechos fundamentales frente a los avances tecnológicos en la era digital.

II. LA EQUÍVOCA CONSTITUCIONALIZACIÓN DE «LA INFORMÁTICA»

El constituyente de 1978 adoptó decisiones que, sin duda, ubicaron el texto constitucional en la vanguardia de las normas fundamentales de su tiempo. Lejos de consagrar previsiones clásicas y atemporales, la Constitución se hizo eco de las transformaciones sociales de su tiempo aun cuando su devenir histórico resultara aún incierto. Es el caso de la consagración en su artículo 18.4 del fenómeno informático: «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

El artículo 18.4 CE ha merecido un indudable reconocimiento por tratarse de un loable intento de actualización y adecuación de la normativa constitucional a las nuevas realidades sociales que afectaban al ser humano en su dignidad y en el disfrute de sus derechos[10]. Sin embargo, esta positiva apreciación no puede estar exenta de una valoración sobre las lagunas e interrogantes que se cernían sobre la literalidad de un precepto que necesitó de un desarrollo legal y jurisprudencial para su correcto entendimiento.

El artículo 18.4 CE, lejos de explicitar un singular derecho o libertad, formula un mandato al legislador notablemente abierto: establecer límites al uso de la informática con la finalidad de proteger y preservar el pleno ejercicio de determinados derechos fundamentales potencialmente en riesgo (honor e intimidad).

Sin lugar a dudas, el constituyente partía del prejuicio negativo hacia el impacto de la informática no tanto en la vida de los ciudadanos como en el disfrute de sus derechos fundamentales. El «uso de la informática» ya había ofrecido suficientes ejemplos en la sociedad del momento de intentos de injerencia en la vida privada de los individuos por parte de los poderes públicos —tanto en los regímenes dictatoriales próximos a extinguirse como en las más reconocidas democracias occidentales— como para atender estas alertas y darles una respuesta normativa.

[10] Pérez Luño, A. E. (1979): «La protección de la intimidad frente a la informática en la Constitución española de 1978», *Revista de Estudios Políticos*, núm. 9, pp. 59 a 71.

El intenso proceso de informatización alemán inaugurado en la década de sesenta fue seguido de un específico desarrollo legislativo con la aprobación a inicios de los setenta de leyes de los Lander que regulaban los centros de procesamiento de datos de las administraciones públicas en Schleswig-Holstein, Baviera, Renania-Palatinado, Renania del Norte-Westfalia o Baden-Württemberg. Estas normas regulaban la actividad informática de las Administraciones Públicas y empezaron a establecer límites a su uso garantizando la confidencialidad en el tratamiento automatizado de datos e, incluso, llegando a consagrar en la ley de Hesse de 1970 un derecho a la protección de datos [11]. La década de los setenta conoció la proliferación de normas estatales dirigidas a proteger la privacidad y los datos personales frente al uso de la informática en Suecia (1973), Estados Unidos (1974), Alemania (1977), Austria, Dinamarca, Noruega y Francia (1978). Este intenso desarrollo legislativo europeo obedece a una lógica similar: la creación de bases de datos personales de carácter público que eran percibidas socialmente como instrumentos de control que podían poner en riesgo la intimidad y el honor de las personas. El caso francés resulta paradigmático: el Ministerio del Interior desarrolló en secreto a principios de los setenta una iniciativa denominada SAFARI (*«Système automatisé pour los fichiers administratifs et le répertoire des individus»*) consistente en informatizar datos personales a partir de un número único de identificación personal y que avocó a la creación de la *Commission Nationale de l'Informatique et des Libertés* (CNIL) y a la aprobación de la Ley 78-17, de 6 de enero de 1978 *(«Loi relative à l'informatique, aux fichiers et aux libertés»)* [12].

Este contexto fue decisivo, sin duda, para que la Constitución portuguesa de 1976 consagrara, por primera vez en la historia constitucional, un precepto dedicado a *la utilización de la informática* en los siguientes términos: «1. Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma

[11] Pascual Huerta, P. (2017): *La génesis del derecho fundamental a la protección de datos personales*, Tesis doctoral, Universidad Complutense, Madrid (http://eprints.ucm.es/43050/1/T38862.pdf).

[12] Da buena cuenta de la atención de los constituyentes españoles al contexto conflictual comparado la referencia del Diputado Martín Toval al Caso SAFARI acaecido en Francia: «recuérdese el precedente del programa «Safari» (es curioso el nombre que se le puso, debió de ser por aquello de la caza), preparado por el Ministro del Interior francés hace aproximadamente tres años que pretendía el control personal de todos los ciudadanos a través del establecimiento de códigos con datos personales y familiares, estudios y calificaciones obtenidas, vida profesional, multas, sanciones, despidos, afiliación política y sindical, etc… Es evidente que existe una tendencia objetiva hacia la autorización creciente de la informática, penetrando en el dominio de lo que debe ser estrictamente la esfera de la privacidad» (Cortes Generales: *Constitución española. Trabajos parlamentarios*, Tomo I, Madrid, Cortes Generales, 1980, p. 1070).

de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización. 2. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos. 3. Se prohíbe atribuir un numero nacional único a los ciudadanos» (art. 35). El constituyente portugués sintetizó las preocupaciones de su tiempo en dos planos: 1) prohibiendo la existencia de registros públicos que pudieran afectar a la libertad ideológica o religiosa o que permitieran invadir la privacidad de los individuos mediante identificación numérica personal; 2) y consagrando los perfiles básicos del novedoso derecho a la protección de datos mediante el reconocimiento del derecho de acceso a los registros y a la rectificación de los datos personales.

Al igual que ocurrió en otros ámbitos, resulta pacífico —más bien evidente— admitir que este precepto de la Constitución portuguesa influyó al constituyente español al redactar el artículo 18.4 CE aunque debe reconocerse que con una ambición notablemente inferior. La Constitución española se limitó a reconocer los riesgos de la informática y a obligar al legislador a imponer una limitación de uso pero sin delimitar contornos específicos de ese desarrollo legislativo ni consagrar expresamente un derecho constitucional a la protección de datos frente al uso de la informática. Pero resulta evidente —como tiempo después reconocería el Tribunal Constitucional— que el artículo 18.4 CE solo podía adquirir pleno sentido relacionándolo con las fuentes de Derecho Comparado de las que había bebido. En definitiva, a pesar de su silencio y de su apertura hermenéutica, este precepto venía a consagrar el derecho a la protección de datos cuya gestación se había producido en Europa desde comienzos de la década y cuya consolidación había tenido lugar mediante numerosas leyes nacionales e, incluso, el texto constitucional portugués.

Pero, por si todavía se albergaran dudas sobre el alcance y significado del artículo 18.4 CE, el iter constituyente las despeja.

De la preocupación del constituyente sobre los riesgos de la informática para el disfrute de los derechos fundamentales dan buena cuenta numerosas intervenciones en los debates constituyentes: «se corre el peligro en este momento de que la informática se use de forma desmesurada para aportación de datos, etc. Pero sucede que en el futuro puede haber otros medios; la informática es solo un medio técnico … no entiendo por qué hay que hacer una mención expresa a la informática y no a otra serie de técnicas o medios que también pueden ir contra la intimidad personal y familiar y contra el honor de los ciudadanos» (Sancho Rof, UCD); «mi Grupo votará favorablemente todo aquello que signifique incluir limitaciones de la informática» (Martín Toval, Grupo Socialista); «el

tema de la informática es fundamental, aunque hoy solo se encuentre en los inicios … eso debemos dar una referencia explícita... Se trata de establecer garantías de control de los controladores» (Solé Tura, Grupo Comunista); «tenemos que situarnos en el futuro … vendrán otras muchas técnicas -no solo la informática-, y resulta imprescindible prevenir y prepararnos para ellas adecuadamente y no quedarnos desplazados en la carrera, aun antes de haber salido de la meta … El mundo y las personas están cambiando a ritmo inimaginables. Hemos de prepararnos para entender este mundo y proteger los derechos de los ciudadanos en los ambientes individuales, familiar y social …Hay que evitar la traición de la tecnología; hay que arbitrar nuevos sistemas de valores» (Zarazaga, Grupo Mixto)[13]. La insatisfacción de los constituyentes por la limitada referencia a «la informática» resultó reiterada. Los riesgos a los que potencialmente se verían sometidos los derechos fundamentales de los ciudadanos no solo procederían de la existencia de bases de datos informatizadas si no del conjunto de nuevas tecnologías de amplio alcance.

Aunque el texto definitivo del artículo 18.1 no incorporara un expreso reconocimiento del derecho a la protección de datos —como sí hizo el artículo 35 de la Constitución portuguesa — resulta evidente que estuvo presente en los debates esta hipótesis. La siguiente enmienda alternativa del Grupo Mixto lo pone de manifiesto: «la ley regulará el acopio, uso y difusión de los datos personales contenidos en los archivos o registros, susceptibles de acceso automático, con el objeto de garantizar las libertades públicas y el ordenamiento constitucional» [14].

Tampoco resulta desdeñable el reiterado intento de algunos grupos parlamentarios por suprimir este apartado cuarto del artículo 18 CE entendiendo que su existencia constituiría una mera reiteración de la plena garantía que ya otorgaba el artículo 18.1 a los derechos al honor y a la intimidad. Como ha venido ocurriendo a lo largo de las últimas cuatro décadas, la plena autonomización del derecho a la protección de datos respecto del derecho a la intimidad ya resultó en origen dificultosa. Habría que esperar al impulso de las normas europeas trascendentales (Convenio 108 del Consejo de Europa y Directiva 95/46) para que la arquitectura de un derecho fundamental autónomo a la protección de datos ofreciera unos perfiles dogmáticos suficientemente definidos.

[13] Cortes Generales: *Constitución española. Trabajos parlamentarios*, Tomo I, Madrid, Cortes Generales, 1980, pp. 1068 y ss.

[14] Cortes Generales: *Constitución española. Trabajos parlamentarios*, Tomo I, Madrid, Cortes Generales, 1980, p. 321.

III. EL CONVENIO 108 DEL CONSEJO DE EUROPA (1981)

España no ratificó hasta el 27 de enero de 1984 —entrando en vigor el 1 de octubre de 1985— el Convenio 108 del Consejo de Europa de 28 de enero de 1981 *para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*. Sin embargo, no cuesta imaginar que el proceso de gestación del que acabaría siendo el primer instrumento internacional jurídicamente vinculante en el ámbito de la protección de datos se inició suficiente tiempo atrás para ubicarse en el contexto temporal en el que los constituyentes españoles apostaron por constitucionalizar el artículo 18.4 CE. Una razón adicional para considerar razonable el anclaje en el artículo 18.4 CE del derecho a la protección de datos personales frente al uso de la informática.

El Convenio 108 buscaba ampliar la protección de los derechos y de las libertades fundamentales —particularmente, la privacidad— frente a la intensificación de la circulación trasfronteriza de los datos de carácter personal objeto de tratamiento automatizado y estableció un marco de referencia preciso para el desarrollo del artículo 18.4 CE.

El Convenio 108 pretendía garantizar a cualquier persona física el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal estableciendo una definición de «dato de carácter personal» que perduraría a lo largo de las siguientes décadas —«cualquier información relativa a una persona física identificada o identificable»— y extendiendo el ámbito de protección no solo a los ficheros si no, también, a los «tratamientos automatizados» —«cualesquiera operaciones automatizadas como el registro de datos, operaciones lógicas aritméticas, modificación, borrado, extracción o difusión»—. En consecuencia, el Convenio 108 se aplicaría a todos los ficheros y a los tratamientos automatizados de datos de carácter personal tanto en el sector público como privado. Esto es, los miedos originales sobre los registros públicos dieron paso a la necesidad de garantizar la protección de datos también frente a los tratamientos automatizados del sector privado.

El Convenio 108 contenía los principios básicos para la protección de datos que han presidido la forja de este derecho durante las últimas décadas: 1.º) *Calidad de los datos*. Los datos de carácter personal objeto de tratamiento automatizado deberían: a) obtenerse y tratarse leal y legítimamente registrándose para finalidades determinadas y legítimas, y no utilizándose de forma incompatible con dichas finalidades; b) ser adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hubieran registrado; c) ser exactos y actualizados; d) conservándose exclusivamente durante el tiempo necesario para las

finalidades para las cuales se hubieran registrado. 2.º) *Datos sensibles*. Los datos que revelasen origen racial, opiniones políticas, convicciones religiosas u otras convicciones, y los relativos a condenas penales, a la salud o a la vida sexual, no podrían tratarse automáticamente salvo con las garantías apropiadas. 3.º) *Seguridad de los datos*. Deberían adoptarse las medidas de seguridad apropiadas para la protección de datos registrados en ficheros automatizados para evitar su destrucción o pérdida accidental y el acceso, modificación o difusión no autorizados. 4.º) *Derechos de acceso, rectificación y cancelación*. Cualquier persona tendría derecho a: a) obtener a intervalos razonables, sin demora ni gastos excesivos la confirmación de la existencia de ficheros automatizados de datos que le conciernan y la comunicación de dichos datos en forma inteligible; b) la rectificación o borrado de dichos datos cuando se hubieran tratado infringiendo estos principios básicos; c) y disponer de un recurso de no atenderse las peticiones anteriores. Las *limitaciones* a los principios y derechos anteriores únicamente podrían referirse a: a) la seguridad del Estado, la seguridad pública, los intereses monetarios del Estado o la represión de infracciones penales; b) ficheros automatizados de datos para fines estadísticos o de investigación científica. Los Estados se comprometían a establecer sanciones y recursos contra las infracciones de los principios básicos para la protección de datos.

IV. EL DERECHO DE PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL AUTÓNOMO

La mayor parte de los ordenamientos jurídicos de nuestro entorno otorgan a la protección de datos personales la naturaleza de derecho y, en nuestro sistema jurídico, el Tribunal Constitucional le ha reconocido rango de derecho fundamental, autónomo del derecho a la intimidad, a partir de la expresa referencia contenida en el artículo 18.4 de la Constitución.

Aunque inicialmente[15] el Tribunal Constitucional calificaba este derecho como una especificación del derecho a la intimidad, pronto le otorgó la naturaleza de un derecho fundamental autónomo.

En su Sentencia 254/93, el Tribunal Constitucional proclamó lo que sigue: «nuestra CE ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron ori-

[15] Lucas Murillo de la Cueva, P. (2003): «La primera jurisprudencia sobre el derecho a la autodeterminación informativa», Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid, núm. 1.

ginándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la CE llama "la informática"». Esto es, el TC no limita el alcance protector del artículo 18.4 CE a su vinculación con los derechos al honor y a la intimidad, ya que lo expande al otorgarle carácter autónomo caracterizándolo como *un derecho fundamental frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos* [16].

En ausencia de un desarrollo legislativo del artículo 18.4 CE, el TC advierte que no nos hallamos ante un mero mandato dirigido al legislador sin virtualidad para amparar por sí mismo pretensiones individuales por no ser meros principios programáticos. En ausencia de desarrollo legislativo este mandato constitucional tendría un contenido mínimo. El TC se interroga sobre dicho contenido mínimo y, aunque admite una aproximación negativa reconociendo un límite en el respeto al honor y la intimidad, concluye: «la efectividad de ese derecho puede requerir inexcusablemente de alguna garantía complementaria, y es aquí donde pueden venir en auxilio interpretativo los tratados y convenios internacionales sobre esta materia suscritos por España … la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada «libertad informática», es así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático *(habeas data)»*. En consecuencia, el TC admite el Convenio 108 del Consejo de Europa como referencia interpretativa: «la realidad de los problemas a los que se enfrentó la elaboración y la ratificación de dicho tratado internacional, así como la experiencia de los países del Consejo de Europa que ha sido condensada en su articulado, llevan a la conclusión de que la protección de la intimidad de los ciudadanos requiere que éstos puedan conocer la existencia y los rasgos de aquellos ficheros automatizados donde las Administraciones Públicas conservan datos de carácter personal que les conciernen, así como cuáles son esos datos personales en poder de las autoridades».

De las limitaciones del derecho a la intimidad para afrontar los riesgos provenientes de las nuevas tecnologías da cuenta la siguiente afirmación del TC:

[16] Villaverde Menéndez, I. (1994): «Protección de Datos Personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993», *Revista Española de Derecho Constitucional,* núm 41, pp. 187 a 224.

«Esta constatación elemental de que los datos personales que almacena la Administración son utilizados por sus autoridades y sus servicios impide aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración Pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el artículo 18 CE, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos». Sin embargo, la STC 254/93 todavía imbrica notablemente la protección de datos personales en el derecho fundamental a la intimidad: «al negarse a comunicarle la existencia e identificación de los ficheros automatizados que mantiene con datos de carácter personal, así como los datos que le conciernen a él personalmente, la Administración demandada en este proceso vulneró el contenido esencial del derecho a la intimidad».

Habrá que esperar a las SSTC 290/2000 y 292/2000 para obtener un pronunciamiento inequívoco y concluyente del Tribunal Constitucional [17].

El artículo 18.4 CE ha servido al Tribunal constitucional para, partiendo de la consagración de la «dignidad humana como fundamento del orden político y de la paz social» (art. 10.1 CE), proclamar la existencia de un derecho fundamental, autónomo del derecho a la intimidad y con un contenido esencial propio que lo define y caracteriza.

La STC 290/2000, de 30 de noviembre, reiteró pronunciamientos previos insistiendo en que el derecho consagrado en el artículo 18.4 de la Constitución contenía un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos pero, además, constituía, en sí mismo, un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama la informática. Esta Sentencia da un salto cualitativo al proclamar lo que sigue: «el derecho fundamental al que estamos haciendo referencia garantiza a la persona un poder de control y disposición sobre sus datos personales. Pues confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como

[17] Alguacil González Aurioles, J. (2001): «La libertad informática: aspectos sustantivos y competenciales (SSTC 290 y 292/2000)», *Teoría y Realidad Constitucional*, núm. 7, pp. 365 a 385.

el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos. En suma, el derecho fundamental comprende un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos. De suerte que es sobre dichos ficheros donde han de proyectarse, en última instancia, las medidas destinadas a la salvaguardia del derecho fundamental aquí considerado por parte de las Administraciones Públicas competentes».

Pero será la STC 292/2000 de 30 de noviembre, la que cerrará el círculo de la autonomización del derecho a la protección de datos respecto del derecho a la intimidad reconociéndole, además, un contenido esencial: «el derecho fundamental a la protección de datos persigue garantizar a la persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado, y que no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que el artículo 18.1 CE otorga, sino los datos de carácter personal». Y concluye: «la peculiaridad de este derecho fundamental a la protección de datos respecto del derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran».

En consecuencia, al establecer el carácter independiente y autónomo del derecho, el Tribunal garantiza, no solo un ámbito de protección específico del derecho a la protección de datos de carácter personal, sino también un ámbito más idóneo —que el que podían ofrecer, por sí mismos, los derechos fundamentales al honor, a la intimidad y a la propia imagen reconocidos en el artículo 18 CE— ante la eclosión de nuevos peligros que las nuevas tecnologías pueden suponer.

V. LA LORTAD (1992), LA LOPD (1999) Y SU REFORMA (2011)

Si bien el derecho fundamental a la autodeterminación informativa[18] (más conocido, entre nosotros, como derecho a la protección de datos de carácter personal) se incorporó al ordenamiento español como consecuencia de la ratificación

[18] Martínez, R. (2004): *Una aproximación crítica a la autodeterminación informativa*, Civitas, Pamplona.

del Convenio 108 del Consejo de Europa de 1981, el primer texto legislativo que lo reguló, desarrollando el artículo 18.4 de la Constitución, fue la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD)[19].

Sin embargo, la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, amplió el ámbito de protección del derecho a todo tipo de tratamiento de datos personales, automatizado o no. Finalmente, para trasponer dicha Directiva, se aprobó la Ley Orgánica 15/1999, de 13 de diciembre de Protección de datos de carácter personal (LOPD), que derogó la LORTAD y cuyo objeto se extendió a «garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal»[20].

Finalmente, la LOPD fue desarrollada reglamentariamente mediante el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprobó el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal [21]. Con anterioridad, el Real Decreto 428/1993, de 26 de marzo, aprobó el Estatuto de la Agencia de Protección de Datos. Debe tenerse en cuenta que numerosas leyes sectoriales ——como es el caso, por ejemplo, de la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones— amplían el ámbito de competencias de la Agencia Española de Protección de Datos (AEPD).

La LOPD define «dato personal» como «cualquier información concerniente a personas físicas identificadas o identificables» (art. 3) y el RLOPD extiende su alcance y casuística: «cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables» (art. 5 f). Estrechamente vinculado al concepto anterior aparece el de «persona identificable», de forma que se considera como tal aquélla que resulta identificable sin «plazos o actividades desproporcionados».

---

[19] Lucas Murillo de la Cueva, P. (1993): *Informática y protección de datos personales,* Centro de Estudios Constitucionales, Madrid.

[20] Lesmes Serrano, C. (2008): *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia* (Coord.) Valladolid, Lex Nova; Troncoso Reigada, A. (2010*): Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Cizur Menor (Navarra), Thomson-Reuters.

[21] Martínez Martínez, R. (2009): *Protección de Datos. Comentarios al Reglamento de Desarrollo de la LOPD*, (director), Valencia. Tirant lo Blanch; Zabía de la Mata, J. (2008): *Protección de Datos. Comentarios al Reglamento* (director), Valladolid, Lex Nova.

Nombre, apellidos y domicilio son datos personales por excelencia, pero, desde luego, no son los únicos. Así, por ejemplo, el artículo 7 LOPD contempla una categoría especial cuales son los «datos especialmente protegidos»; a saber, los que hacen referencia al origen racial, a la salud y a la vida sexual. Otros datos personales (documento nacional de identidad, número de teléfono, dirección de correo electrónico, matrículas de automóviles, la imagen, o las direcciones IPs de Internet) no resultan, a priori, de tan pacífica configuración a pesar de que, en la mayoría de las ocasiones, permiten inequívocamente la identificación de personas físicas. Ahora bien, no cualquier dato personal es objeto de protección por la legislación vigente pues ésta circunscribe su ámbito de aplicación: «La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado» (art. 1 LOPD).

En su Título II, la LOPD contiene los principios fundamentales del régimen de protección de datos. 1) El *principio de calidad* de datos, consagrado en el artículo 4 LOPD, integra, a su vez, los principios de proporcionalidad, finalidad, veracidad y exactitud, que obligan a la cancelación y sustitución de oficio en el caso de inexactitud y amparan el ejercicio de los derechos instrumentales de protección de datos (acceso, rectificación, cancelación y oposición). 2) El *principio de proporcionalidad*, en íntima conexión con el de finalidad, impone la necesidad de que medie una nítida conexión entre la información personal que se recaba y trata informáticamente y el legítimo objetivo para el que se solicita. Ello implica la adecuación, pertinencia y ponderación en relación con el fin para el que la información se recaba y, en consecuencia, proscribe el uso de los datos para finalidades distintas a las que motivaron su recogida. En el caso de que la recogida de datos se haya realizado para unos fines determinados, cualquier uso o tratamiento posterior que no esté en consonancia con las finalidades para las que fueron facilitados y sobre las que el afectado no consintió, resulta incompatible con la finalidad que determinó la entrega. Los principios de veracidad y exactitud obligan a que los datos recabados sean exactos y actualizados. 3) El *principio de consentimiento* es la clave de bóveda del sistema de protección de datos. Se sustancia habilitando a la persona física a ejercer el control sobre sus datos de carácter personal y explica la recurrente denominación del derecho fundamental a la protección de datos personales como derecho a la «autodeterminación informativa». Según el artículo 6.1 LOPD, «el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa». No obstante, la LOPD admite excepciones cuando los datos de carácter personal son recabados para el ejercicio de las funciones propias de

las Administraciones públicas en el ámbito de sus competencias, cuando se refieren a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento, cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado, cuando los datos figuren en fuentes accesibles al público y cuando su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos. 4) El *deber de información* no tiene menos trascendencia que los anteriores, pues es el presupuesto que permite llevar a cabo el ejercicio del derecho. A tenor del artículo 5 LOPD, los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco de datos tales como la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. Asimismo, la información debe arrojar luz sobre las consecuencias de la obtención de los datos o de la negativa a suministrarlos, además de identificar al responsable del tratamiento o, en su caso, de su representante.

La STC 292/2002 establecía que el derecho fundamental a la protección de datos «atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley». Estas facultades se instrumentan a través de los derechos que la regulación de protección de datos reconoce. Los derechos instrumentales de protección de datos se regulan en el Título III de la LOPD (arts. 13 a 19) y en su Reglamento de desarrollo. Los derechos de protección de datos (acceso, rectificación, cancelación y oposición) tienen carácter personalísimo y solo pueden ser ejercidos por el afectado cuando éste acredite su identidad, o por su representante legal cuando éste acredite encontrarse en situación de incapacidad o minoría de edad que le imposibilite su ejercicio personal. Estos derechos poseen carácter gratuito e independiente, de forma que no cabe entender que el ejercicio de uno deba constituir un requisito para el ejercicio de otro. El responsable del fichero o tratamiento «deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aun cuando el mismo no hubiese utilizado el procedimiento establecido» (art. 24 RLOPD). El *derecho de acceso* posibilita que el afectado pueda obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, o la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos. Los *derechos de rectificación y cancelación* atribuyen la facultad, respectivamente, de solicitar que los datos sean modificados cuando resulten inexactos o incompletos, o que se supriman éstos

cuando sean inadecuados, excesivos o se haya agotado la finalidad para la que se recabaron. El *derecho de oposición* asiste al afectado cuando su pretensión estriba en que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo cuando concurra un motivo legítimo y fundado, referido a su concreta situación personal que lo justifique.

Una de las singulares innovaciones de la normativa de protección de datos consistió en atribuir la garantía del derecho a una Administración independiente. La Agencia Española de Protección de Datos (AEPD) es un ente de Derecho público, que actúa con independencia, con personalidad jurídica propia y plena capacidad pública y privada. La AEPD extiende su competencia al conjunto del territorio nacional —como proclamó la STC 290/2000, «la exigencia constitucional de protección de los derechos fundamentales se extiende a todo el territorio nacional» por lo que «las funciones y potestades de este órgano han de ejercerse cualquiera que sea el lugar del territorio nacional donde se encuentren los ficheros automatizados conteniendo datos de carácter personal y sean quienes sean los responsables de tales ficheros»— y se coordina con las Agencias Autonómicas de Protección de datos existentes [22]. La AEPD extiende su competencia al control de los ficheros de titularidad privada y a los de titularidad pública de la Administración General del Estado, de las Administraciones Autonómicas y Locales (excepto en aquellas Comunidades Autónomas que cuentan con Agencias de Protección de Datos propias).

La Agencia Española de Protección de Datos es una autoridad de control encargada de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos. La AEPD, que tiene ya 25 años de existencia, va a actuar en el ejercicio de sus funciones con plena independencia de las Administraciones Públicas. Sin embargo, no es misión exclusiva de la AEPD la de perseguir los incumplimientos de la norma, sino principalmente la de instruir, divulgar y crear conciencia de que del cumplimiento de dichas normas se deducen importantes beneficios para las personas, individualmente consideradas, y también para la comunidad en su conjunto.

[22] Hasta la fecha, cuatro CC.AA. crearon sus propias Autoridades de Protección de Datos autonómicas: Madrid, a través de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid (derogada en 2011 y suprimida la Agencia de la Comunidad de Madrid a partir del 1 de enero de 2012). Cataluña, por la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos. País Vasco, mediante Ley 2/2004, de 25 de febrero, de Ficheros de Datos de carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos. Andalucía, por Ley 1/2014, de 25 de junio, de Transparencia Pública de Andalucía.

Entre las funciones de la AEPD destaca la de investigar las posibles infracciones de datos e imponer las sanciones previstas en las normas sobre protección de datos. La AEPD está obligada a tomar en consideración todas las denuncias o reclamaciones que recibe, realizando las investigaciones encaminadas a determinar si se ha producido o no una violación de los principios de la LOPD o se ha denegado o impedido el ejercicio de los derechos de acceso, rectificación, cancelación y oposición [23].

Durante los últimos veinticinco años, España ha sido el ejemplo recurrente de sistema sancionador por incumplimiento de la legislación de protección de datos más exigente de Europa. La garantía efectiva de la legislación española de protección de datos se ha construido sobre la aplicación de un régimen sancionador (multas) al sector privado extraordinariamente duro [24]. El origen de este sistema sancionador se encuentra en la primera ley española de protección de datos: Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD). Durante más de dos décadas, han perdurado inalterados buena parte de los rasgos básicos del régimen sancionador diseñado por la LORTAD.

La LORTD estableció una gradación en las multas que la AEPD podía imponer al sector privado (empresas y organizaciones privadas) que ha permanecido casi intacta hasta la fecha y que resultan las más elevadas de Europa: a) Infracciones leves: de 600 (hoy, tras la reforma de 2011, 900) a 60.001 €; b) Infracciones graves: de 60.001 (hoy, 40.001) a 300.000 €; c) Infracciones muy graves: 300.001 a 600.000 €. No en vano, durante la última década, la AEPD ha impuesto un total de *más de 206 millones de euros en multas* [25]. La reforma del régimen sancionador previsto en la legislación de protección de datos (primero, en la LORTAD y, después, en la LOPD) venía siendo, durante casi una década, incisivamente demandada por diversas organizaciones empresariales —particularmente, del sector de la publicidad y el marketing como principales destinatarias de sus rigurosas multas y alegando los elevados costes de su cumplimiento y la desventaja competitiva que les provocaba frente a similares sectores

[23] AA.VV. (2008): *La potestad sancionadora de la Agencia Española de Protección de Datos,* Cizur Menor (Navarra), AEPD-Aranzadi.

[24] Sirva como ejemplo, la Resolución sancionadora de la AEPD 2892/2013 por la que se imponía a Google Inc. una multa de 900.000 € por la unificación de sus políticas de privacidad en 2012. Idénticos hechos merecieron que la CNIL francesa impusiera a Google el 8 de enero de 2014 una multa de solo 150.000 €.

[25] Rallo Lombarte, A. (2014): «Estudio sobre la evolución del régimen sancionador en la legislación de protección de datos», *Revista de Estudios Políticos*, núm. 166, octubre-diciembre, pp. 95 a 121.

empresariales de otros países europeos—. La Disposición Final 56 de la Ley 2/2011, de 4 de marzo, de Economía Sostenible atendió la demanda anterior y reformó los artículos 43 a 46 y 49 LOPD. El régimen sancionador español se había caracterizado históricamente por la elevada cuantía de sus sanciones económicas y una devaluación significativa de éstas habría enviado un mensaje al conjunto de la sociedad de relajación en la garantía del derecho de protección de datos opuesto a las necesidades sociales hoy existentes. Además, si bien dos décadas atrás cuando se instauró podía pecar de exceso, en la actualidad la realidad socio-económica y los sistemas sancionatorios implantados en países del entorno (Francia o Reino Unido) o en la Unión Europea (como lo evidencian las sanciones económicas contenidas en Reglamento Europeo de Protección de Datos) demuestran su plena vigencia.

VI. LA EUROPEIZACIÓN DEL DERECHO DE PROTECCIÓN DE DATOS: LA DIRECTIVA 95/46, EL ARTÍCULO 8 CDFUE Y EL REGLAMENTO UE 2016/679

La *Directiva* 95/46 estableció un hito en la historia de la protección de los datos personales en la Unión Europea[26].

Dos décadas después, los principios consagrados en la Directiva seguían siendo válidos pero *la rapidez de la evolución tecnológica y la globalización* ofrecían *nuevos retos* en materia de protección de los datos personales. Hoy, la tecnología permite a los ciudadanos intercambiar fácilmente información con respecto a sus comportamientos y sus preferencias, y hacerla pública a nivel mundial a una escala sin precedentes. Las redes sociales[27], con centenares de millones de miembros en todo el mundo, constituyen seguramente el ejemplo más evidente de este fenómeno, sin ser el único. La computación en nube, esto es, informática basada en internet en la que los programas, los recursos compartidos y la información

[26] Arenas Ramiro, M.: *El derecho fundamental a la protección de datos personales en Europa,* Tirant lo Blanch-Agencia Española de Protección de Datos, 2006, Valencia; Rebollo Delgado, L.: *Vida privada y protección de datos en la Unión Europea,* Madrid. 2007, Dykinson; Kuner, C. (2007): *European Data Protection Law. Corporate Compliance and Regulation*, Oxford University Press,, Oxford.

[27] Rallo Lombarte, A. y Martínez, R. (2013): «Data Protection, Social Networks, and Online Mass Media», *European Data Protection: Coming of Age*, Serge Gutwirth, Ronald Leenes, Paul De Hert and Yves Poullet Editors, ed. Springer, London-New York, pp. 407 a 423. Rallo, A. (2013): «La protección de la privacidad en las redes sociales de Internet: la experiencia canadiense con facebook, google y otros», *Derecho y Redes Sociales*, Artemi Rallo Lombarte y Ricard Martínez Martínez, Editores, 2.ª edición, ed. Civitas-Thomson Reuters, Pamplona, pp. 257 a 284.

se encuentran en servidores remotos, también plantean retos para la protección de datos, dado que puede implicar la pérdida del control por parte de los individuos de su información potencialmente sensible cuando almacenan sus datos utilizando programas alojados en servidores ajenos. Los métodos de recogida de los datos personales son cada vez más complicados y se detectan con más dificultad. El mayor recurso a procedimientos que permiten la recogida automática de datos, como el pago electrónico de billetes, el cobro de peajes en carreteras, o instrumentos de geolocalización, facilitan la ubicación de un individuo por el mero uso por su parte de un dispositivo móvil.

Las consideraciones anteriores plantearon retos que la normativa europea de protección de datos debía acometer: el impacto de las nuevas tecnologías, el reforzamiento del mercado interior de la protección de datos, la globalización y la mejora de las transferencias internacionales de datos, la aplicación efectiva de las normas sobre protección de datos y la coherencia del marco jurídico europeo regulador de la protección de datos. Los retos mencionados invitaban a la UE a elaborar una normativa europea, global y coherente que garantizara el pleno respeto del derecho fundamental a la protección de los datos personales.

Además, desde que se adoptó la Directiva 95/46, la Unión Europea había conocido importantes novedades jurídico-constitucionales. En 2000 se proclamó en Niza la CDFUE que, en su artículo 8, reconocía el derecho a *la protección de datos personales*: «1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente». Posteriormente, el 12 de diciembre de 2007 esta redacción quedó confirmada en Estrasburgo y, finalmente, el artículo 6 del Tratado de la Unión Europea (TUE) —en la redacción consolidada por el Tratado de Lisboa— le otorgó el *mismo valor jurídico* que a los Tratados.

La mejor demostración de esta historia de éxito protagonizada por la Directiva 95/46 reside en su capacidad de, en poco más de una década, consolidar constitucionalmente en los Tratados constitutivos (ex artículo 6 TUE, artículo 8 CDFUE y artículo 16 TFUE) un derecho emergente a la protección de datos personales cuyos orígenes se remontan apenas a 1981 con la adopción del Convenio del Consejo de Europa para la protección de datos personales frente a su tratamiento automatizado.

En consecuencia, el Tratado de Lisboa otorgó fuerza jurídica vinculante a la CDFUE y, en concreto, al derecho autónomo a la protección de datos de carác-

ter personal que consagra en su artículo 8. Los artículos 6 TUE, 8 CDFUE y 16 TFUE crearon una *nueva base jurídica* para la elaboración de una normativa global de la Unión Europea sobre protección de datos personales [28].

El Reglamento 2016/679 General de Protección de Datos (REPD) [29] dio respuesta a las insistentes críticas que soportó la Directiva 95/46: la fragmentación de la protección de datos personales que urgía mayor seguridad jurídica mediante la armonización de las normas de protección de los datos. La complejidad de esta normativa en materia de transferencias internacionales de datos personales constituía un impedimento sustancial en una economía planetariamente globalizada. El Reglamento UE 2016/679 constituyó el instrumento jurídico idóneo para regular el derecho a la protección de datos personales dada su aplicabilidad directa.

La verdadera armonización de la normativa europea de protección de datos exigía un régimen sancionador común. La Directiva 95/46 apenas imponía a los Estados la obligación de adoptar medidas adecuadas para garantizar su plena aplicación pero este mandato se tradujo en una pavorosa asimetría europea sobre la que, sin duda, se ha construido una *doble velocidad europea.* Siendo bien escasos los Estados que contemplaban un régimen sancionador económico disuasorio —a la cabeza España—, la realidad europea general mostraba un páramo de flagrante impunidad ante las infracciones crecientes. Por ello, el REPD refuerza el régimen de sanciones mediante su generalización en todo el territorio de la Unión Europea y mediante un sistema de sanciones efectivas, proporcionadas, disuasorias y potencialmente millonarias. El importe de las multas se fijará teniendo en cuenta la naturaleza, gravedad y duración de la infracción, la intencionalidad o negligencia en la infracción, el grado de responsabilidad de la persona física o jurídica, la reincidencia, las medidas de carácter técnico y organizativo y los procedimientos aplicados por los responsables, el grado de cooperación con la autoridad de control para reparar la infracción.

El tsunami tecnológico que vive la sociedad actual constituyó una de las principales preocupaciones del legislador europeo. Desde que se aprobó la Directiva 95/46, la sociedad de la información y del conocimiento ha adquirido un desarrollo inimaginable y ha provocado un impacto insospechado dos décadas atrás en el flujo de información personal. Las categorías tradicionales sobre las que se asienta el derecho a la protección de datos han evidenciado su debilidad

[28] Rallo Lombarte, A. y García Mahamut, R. (eds.): *Hacia un nuevo derecho europeo de protección de datos. Towards a new European Data Protection Regime*, Tirant lo Blanch, Valencia, 2015.

[29] López Calvo, J. (2017): *Comentarios al Reglamento Europeo de Protección de Datos*, Sepin, Madrid.

y exigen una adecuación a los tiempos actuales que constituyen uno de los principales retos del REPD al actualizar su aplicación al nuevo entorno tecnológico y al crear *nuevos derechos digitales*.

El REPD profundiza en las necesidades de *transparencia e información* al ciudadano al asumir que el flujo masivo de datos en el mundo digital y sus dificultades para perseguir y reparar las vulneraciones del derecho a proteger los datos requiere una mejora extraordinaria en los procesos de otorgamiento del consentimiento. La *infancia* constituye un grupo social sometido a un especial riesgo en el mundo *online* a causa de su masivo acceso a Internet[30] y de la obtusidad de sus reglas y políticas de privacidad. Por ello, el REPD se ocupa de los menores para otorgarles especial protección ante la oferta directa de servicios de la sociedad de la información destinada a los niños. El REPD reconoce, como concreción en el ámbito digital del tradicional derecho de cancelación, el *derecho al olvido*[31], esto es, el derecho de toda persona a la cancelación y no tratamiento de los datos personales cuando ya no sean necesarios para los fines para los que fueron recogidos, cuando los interesados hayan retirado su consentimiento para su tratamiento, cuando se haya agotado el plazo previsto de conservación o cuando se opongan al mismo. Este derecho se estima especialmente aplicable a aquellos supuestos en que los interesados hubieran dado su consentimiento siendo niños, de forma que no fueran enteramente conscientes de los riesgos para su privacidad futura y más tarde quisieran suprimirlos (lo que resulta significativamente más relevante en Internet). Al *derecho olvido* se le oponen, sin embargo, como límites: la libertad de expresión, el interés público relativo a la salud pública, los fines de investigación histórica, estadística y científica y las obligaciones legales europeas o nacionales que impongan la conservación de datos. Un nuevo derecho instrumental de protección de datos aflora, como auténtica novedad, en el REPD: *el derecho a la portabilidad de los datos*. Su alcance no puede entenderse cubierto por el tradicional derecho de acceso sino que ambiciona dar respuesta a una problemática planteada por los más exitosos servicios de la era digital: las redes sociales[32]. El derecho a la portabilidad pretende que, sin dificultades que aborten tal posibilidad, los usuarios de una red social *on line* puedan cancelar sus cuentas

[30] Guerrero Pico, M. C. (2006): *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Thomson-Civitas, Pamplona.

[31] Rallo Lombarte, A. (2014): *El derecho al olvido en Internet. Google versus España*, Centro de Estudios Políticos y Constitucionales, Madrid.

[32] Rallo, A. y Martínez, R. (2010): *Derecho y redes sociales*. Pamplona: Civitas-Thomson Reuters; García Sanz, R. M. (2011): «Redes sociales online: fuentes de acceso público o ficheros de datos personales privados (Aplicación de las Directivas de protección de datos y privacidad en las comunicaciones electrónicas)», *Revista de Derecho Político*, núm. 81, pp. 101 a 154.

abiertas en un concreto portal y trasladar todo el historial generado en su cuenta a una nueva red social. De la trascendencia de este nuevo derecho da buena cuenta una realidad en la que miles de millones de usuarios de redes sociales acumulan en sus cuentas online un auténtico historial de vivencias y relaciones personales y sociales que resultaría abortado si se les negara tal derecho a la portabilidad o generaría un insufrible sometimiento del usuario a los designios de la red social de acogida que resultaría difícilmente conciliable con los estándares básicos de protección de datos y de su misma dignidad. Finalmente, el REPD atiende a la dificultad que la nueva realidad de Internet plantea para *reaccionar jurisdiccionalmente* de forma eficaz frente a las vulneraciones de la normativa de protección de datos protagonizadas por los grandes servicios online que impactan en miles de usuarios los cuales, de forma individual, raramente demandarán a los responsables de dichas infracciones por muy varias razones (limitada relevancia del daño individual, gravosos costes procesales, escasa información y conocimiento del alcance de la infracción, etc.). Por ello, tomando como referencia las *class actions* anglosajonas (singularmente eficaces en el ámbito estadounidense) y al margen de las pertinentes reclamaciones individuales, se reconoce a todo organismo, organización o asociación que tenga por objeto proteger los derechos e intereses de los usuarios y esté debidamente constituida conforme a la legislación nacional el derecho a presentar una *reclamación colectiva* frente una autoridad nacional de control por cuenta de uno o más interesados si considera vulnerados sus derechos. Además, como garantía adicional, los recursos podrán ejercitarse ante los órganos jurisdiccionales del Estado miembro en que el interesado tenga su *residencia habitual*. Todas estas previsiones se unen a las *nuevas reglas sobre legislación aplicable* que extienden la vigencia y aplicabilidad del REPD al tratamiento de datos de individuos residentes en la Unión Europea por parte de *entidades no establecidas en la Unión*, cuando sus actividades persigan ofertar bienes o servicios o hacer un seguimiento del comportamiento de dichos particulares en la Unión. Esto es, el REPD reafirma, por si cupiese duda alguna, su aplicabilidad a todo tratamiento de datos realizado a través de Internet aunque la empresa titular de un determinado servicio (red social, motor de búsqueda, etcétera) tenga su sede en un tercer país (EEUU) y pretende la aplicación de la legislación nacional de este tercer país. Lo que constituye un indiscutible avance en el sistema de garantías procesales del derecho a la protección de datos en la era digital.

Pero, la *Big Data Age* difícilmente encontrará satisfacción a los riesgos que se ciernen sobre la protección de datos a través de mecanismos represores o sancionadores. Por ello, legislador europeo —aun construyendo un exigente y riguroso sistema sancionatorio— ha diseñado una *potente estrategia preventiva* que,

mediante pluralidad de mecanismos e instrumentos, materializa las exigencias básicas del *accountability principle*. El REPD apuesta por la *protección de datos desde el diseño y por defecto* (*Privacy by Design* [33] *and by Default*) al imponer la obligación de garantizar que, por defecto, solo sean objeto de tratamiento los datos personales necesarios para cada fin específico y que solo se recojan y conserven por el tiempo y cantidad mínimos (*data minimization principle*) necesarios para sus fines. El REPD normativiza la práctica preventiva ya presente en sistemas anglosajones (y, singularmente, en el Reino Unido) de las *Evaluaciones de Impacto* en protección de datos —Privacy Impact Assessments (PIAs)[34]— sobre el tratamiento de datos que, por su naturaleza, alcance o fines, entrañen *riesgos específicos*. El REPD crea la figura del *delegado de protección de datos* —de especial predicamento, hasta la fecha, en Alemania y Francia[35]— en todos los organismos públicos y cuando la naturaleza, alcance o fines de una entidad requiera un seguimiento periódico y sistemático. El REPD promociona la autorregulación —*certificaciones y sellos*—. El éxito de la nueva estrategia preventiva diseñada por el REPD dependerá de su eficacia.

Como puede observarse, el origen, evolución y consolidación del derecho a la protección de datos personales tiene una inequívoca impronta europea jalonada por cuatro estadios normativos perfectamente identificables: 1.º) El Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de sus datos de carácter personal. 2.º) La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. 3.º) El artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea al que el Tratado de Lisboa otorgó fuerza jurídica a partir de 2009. 4.º) El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en vigor a partir de mayo de 2018).

Sin embargo, el impacto mundial de esta normativa originariamente europea tiene una innegable doble manifestación: por un lado, en la proliferación de regímenes normativos de protección de los datos personales en el resto de los

[33] Schaar, P. (2010): «Privacy by Design», *Identity in the Information Society*, 3 (2), pp. 267 a 274; Huxtin, P. (2010): «Privacy by Design: Delivering the Promises», *Identity in the Information Society*, 3 (2), pp. 253 a 255.

[34] De obligada consulta, Wright, D. y De Hert, P. (2012): *Privacy Impact Assessment*, Springer, London-New York.

[35] Turk, A. (2011): *La vie privée en peril*, Odile Jacob, Paris.

continentes; y, por otro, en la obligada adecuación de los servicios tecnológicos globales —independientemente de su origen geográfico— a la normativa europea de protección de este derecho fundamental y, en concreto, a la jurisdicción garante de su efectividad, esto es, al Tribunal de Justicia de la Unión Europea (TJUE)[36]. Por ello, hay que afirmar que el TJUE se ha convertido en un auténtico juez garante de la privacidad ante la evolución tecnológica global[37]. La inevitable fuerza expansiva extraterritorial de su jurisprudencia resulta especialmente evidente en algunas de sus sentencias —*Caso Digital Rights* (Directiva conservación de datos), *Caso Google* [38] (derecho al olvido) y *Caso Facebook* (Safe Harbour)— que marcan un hito en la evolución de la protección de los datos personales frente a la globalización tecnológica por su impacto mundial, esto es, por la expansión de los estándares europeos de protección al resto de latitudes del planeta.

La jurisprudencia del TJUE constituye referencia inexcusable pues ilustra sobradamente sobre los enormes riesgos potenciales para la privacidad del individuo que derivan tanto del uso de servicios y dispositivos tecnológicos (telefonía móvil, Internet y redes sociales) en los que se almacena abundante información personal sin que el principio de territorialidad estatal pueda satisfacer las garantías necesarias para evitar la lesión en la intimidad individual.

---

[36] Arenas Ramiro, M. (2006): «El derecho a la protección de datos personales en la jurisprudencia del TJCE», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, vol. 4, p. 95 a 119.

[37] Rallo Lombarte, A. (2017): «El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en Internet», *Teoría y Realidad Constitucional*, núm. 39, pp. 583-610.

[38] Un análisis monográfico de esta STJUE puede encontrarse en Rallo Lombarte, A. (2014): *El derecho al olvido en Internet. Google vs. España…* También, Lucas Murillo de la Cueva, P. (2015): «La distancia y el olvido en la red. Comentario a la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 en el asunto C-131-12», *El juez del derecho administrativo. Libro homenaje a Javier Delgado Barrio,* coord., por Luis Arroyo Jiménez, Margarita Beladíez Rojo, Carlos Ortega Carballo, José María Rodríguez de Santiago; Vilasau, M. (2014): «El caso Google Spain: la afirmación del buscador como responsable del tratamiento y el reconocimiento del derecho al olvido (análisis de la STJUE de 13 de mayo de 2014)», *Revista de Internet, Derecho* y Política, n.º 18; Azurmendi, A. (2015): «Por un derecho al olvido para los europeos: Aportaciones jurisprudenciales de la Sentencia del Tribunal Europeo del Caso Google Spain», *Revista de Derecho Político,* n. 92, enero-abril; Martínez, J. M (2015).: «El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs AEPD y Mario Costeja», *Revista de Derecho Político, n.º* 93, mayo-agosto, pp. 119 y ss.; Martínez, R.(2014): «Aplicar el derecho al olvido», *Revista Aranzadi de derecho y nuevas tecnologías*, n.º 36; Boix Palop, A. (2015): «El equilibrio entre los derechos del artículo 18 de la Constitución, el derecho al olvido y las libertades informativas tras la Sentencia Google», *Revista General de Derecho Administrativo*, n.º 98; Simón, P. (2015): *El reconocimiento del derecho al olvido digital en España y en la UE,* Bosch, Barcelona.

VII. HACIA LA CONSTITUCIONALIZACIÓN DE NUEVOS DERECHOS DIGITALES

La Constitución de 1978 fue pionera en la constitucionalización de garantías frente a los riesgos que acompañaban la revolución tecnológica emergente. La sincrética referencia del artículo 18.4 CE amparó la consagración de un genérico derecho fundamental autónomo a la protección de datos personales.

Resulta de pura justicia reconocer que el decidido impulso de este derecho fundamental ha procedido de instancias europeas hasta el punto que el artículo 8 CDFUE lo elevó a rango constitucional europeo y, a partir del mismo, la Unión Europea ha optado por una inequívoca europeización del derecho de protección de datos a través de su regulación uniforme para toda la Unión Europea mediante el Reglamento Europeo de Protección de Datos. De hecho, la adaptación al Reglamento Europeo de protección de datos, que entrará en vigor el 25 de mayo de 2018, requiere de una nueva ley orgánica que sustituya a la actual LOPD pero de alcance muy limitado pues, aunque el REPD permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros cuando sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, los Estados miembros adoptarán disposiciones nacionales solo para especificar la aplicación del REPD. En definitiva, partiendo de la existencia de un régimen uniforme en toda la Unión, la ley orgánica que reforme la vigente LOPD de 1999 no deberá reiterar el texto del REPD si no clarificar sus disposiciones dentro de los márgenes que éste establece y teniendo en cuenta la propia tradición jurídica nacional.

Sin embargo, el reconocimiento constitucional o europeo, legal o constitucional, del derecho fundamental a la protección de datos no agota la necesidad de establecer un nuevo marco de protección de los ciudadanos en la era digital. Esto es, resulta ineludible la necesidad de reconocer *nuevos derechos digitales* bien en el ámbito legal como constitucional. De nuevo, el ejemplo constitucional portugués constituye una referencia ineludible aunque de escaso alcance. En su dicción actual el artículo 35 de la Constitución portuguesa ofrece un detallado desglose del contenido esencial del derecho a la protección de datos —tomando como referencia, sin duda, el artículo 8 CDFUE— pero sin avanzar en el reconocimiento de otros derechos propios de la era digital: «Utilización de la Informática. 1. Todo ciudadano tendrá derecho de acceso a todos los registros informáticos que le conciernen, a requerir que sean rectificados y actualizados, y a ser informado de la finalidad a que se destinan las informaciones, de conformidad con lo dispuesto en la ley. 2. La ley definirá el concepto de «dato personal», junto con términos y condiciones aplicables a su tratamiento automatizado,

vínculos, transmisiones y uso, y garantizará su protección, en particular por medio de un órgano independiente. 3. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones filosóficas o políticas, afiliaciones a partidos o sindicatos, creencias religiosas, vida privada u orígenes étnicos, salvo con el consentimiento expreso del sujeto, con autorización prevista por la ley y garantías de no discriminación, o con el fin de procesar datos estadísticos que no puedan ser individualmente identificados. 4. El acceso de terceros a los datos personales estará prohibido, salvo en casos excepcionales, de conformidad con la ley. 5. Se prohíbe atribuir un número nacional único a los ciudadanos. 6. Se garantiza a todos el libre acceso a la red informática de uso público. La ley determinará tanto las reglas aplicables al flujo de datos a través de las fronteras como las medidas apropiadas para proteger datos personales y otros que justificadamente hayan de ser salvaguardados en interés nacional. 7. Los datos personales contenidos en archivos manuales disfrutarán de la misma protección prevista en los apartados precedentes, de conformidad con lo dispuesto en la ley».

Lo cierto es que la tecnología constituye una realidad que nos envuelve y que condiciona nuestros comportamientos más cotidianos. Internet es una realidad omnipresente. La transformación digital de nuestra sociedad es una realidad en constante desarrollo. Países como Italia o Francia han aprobado una Declaración de Derechos en Internet o una legislación de impulso digital reforzando los derechos digitales de la ciudadanía[39].

El artículo 18.4 CE —a la vista de la exégesis que hemos expuesto al inicio de este trabajo— evidencia sus limitaciones para atender las necesidades contemporáneas de garantía de los derechos en Internet y ante la Tecnología. Una hipotética reforma de la Constitución debería incluir la actualización de la Constitución a la era digital y constitucionalizar una nueva generación de derechos digitales[40], de carácter sustantivo o prestacional, entre los que merecerían sobresalir los siguientes:

a) El derecho de acceso a Internet independientemente de la condición económica

b) El derecho a la formación digital.

[39] Resolución de Naciones Unidas A/HRC/32/L.20 de 27 de Junio de 2016 sobre *promoción, protección y disfrute de los derechos humanos en Internet*.

[40] Puede consultarse la propuesta programática del PSOE para la constitucionalización de derechos digitales en *Programa Electoral PSOE 2015* (http://www.psoe.es/media-content/2015/11/PSOE_Programa_Electoral_2015.pdf) y la Proposición No de Ley para el reconocimiento de derechos digitales del Grupo Parlamentario Socialista del Congreso de los Diputados publicada el 11 de abril de 2017 en el Boletín Oficial de las Cortes Generales.

c) El derecho a la neutralidad de la Red garantizado un internet libre, abierto, equitativo e innovador.

d) El derecho al honor y a la propia imagen frente a agresiones específicas procedentes de la Red.

e) El derecho a la libertad de expresión y a la veracidad de las informaciones en la Red.

f) El derecho de los trabajadores a su intimidad en la utilización de medios digitales y el derecho a la desconexión laboral

g) El derecho de acceso online a datos, innovaciones, creaciones y conocimiento generado con fondos públicos.

h) El derecho a obtener reparación efectiva ante daños causados por conductas ilícitas en la Red.

i) El derecho de los menores a su seguridad en la Red.

Obviamente, al igual que hace la Constitución portuguesa, no debería perderse la oportunidad de explicitar el contenido mínimo del derecho fundamental a la protección de datos personales reconociendo derechos como los siguientes:

a) El derecho de acceso, rectificación, oposición y cancelación de los datos.
b) El derecho al olvido.
c) El derecho a la seguridad y a la confidencialidad de los datos.
d) El derecho a la portabilidad de los datos.
e) El derecho a la identidad online y a la protección del anonimato.
f) El derecho al patrimonio y testamento digital.

Title:

From «computing freedom» towards the constitutionalization of new digital rights (1978-2018).

Summary

I. Introduction. II. The misleading constitutionalization of «computing». III. Convention 108 of the council of europe (1981). IV. Data protection right as an autonomous fundamental right. V. LORTAD (1992), LOPD (1999) and its reform. VI. The europeanization of data protection right: Directive 95/46, art. 8 CDFUE and

regulation EU 2016/679. VII. Towards the constitutionalization of new digital rights.

Resumen:

La referencia a la informática en la Constitución de 1978 reconoció trascendencia constitucional a la necesidad de protección del individuo frente a los riegos derivados de los avances tecnológicos. Cuatro décadas después, la sociedad contemporánea afronta el reto de constitucionalizar nuevos derechos digitales. En España, sendas leyes (LORTAD y LOPD) desarrollaron el precepto constitucional que consagra la garantía de los derechos frente al uso de la informática. Para preservar a los individuos frente a los riesgos y amenazas de la tecnología, el Tribunal Constitución dedujo del artículo 18.4 CE un derecho fundamental autónomo a la protección de datos personales. Las leyes españolas de protección de datos son el resultado de la obligación de cumplir compromisos internacionales (Convenio 108 del Consejo de Europa de 1981) y europeos (Directiva 95/46, artículo 8 de la CDFUE[41] y Reglamento UE 2016/679). Sin embargo, el reconocimiento constitucional o europeo, legal o constitucional, del derecho fundamental a la protección de datos no agota la necesidad de establecer un nuevo marco de protección de los ciudadanos en la era digital en el que se reconozcan nuevos derechos digitales.

Abstrat:

The reference to computing in the Spanish Constitution (1978) recognized constitutional significance to the need for protection against the technological risks. Four decades later, the contemporary society faces the challenge of constitutionalising new digital rights. In Spain, two laws (LOPD and LORTAD) developed the constitutional article that enshrined the guarantee of rights against the use of computers. The Constitutional Court inferred from article 18.4 CE an autonomous fundamental right to the protection of personal data. Spanish data protection laws are the result of the obligation to comply with international (Convention 108 of the Council of Europe from 1981) and European (Directive 95/46, article 8 of the CDFUE and Regulation EU 2016/679) commitments. However, the European, legal or constitutional, recognition of the fundamental right to data protection does not exclude the need to establish a new framework for the

[41] Guerrero Pico, M. C. (2005): «El derecho fundamental a la protección de los datos de carácter personal en la Constitución Europea», *Revista de Derecho Constitucional Europeo*, núm. 4, pp. 293 a 334.

protection of citizens in the digital age in which new digital rights should be recognized.

Palabras clave:

Protección de datos, intimidad, derechos digitales, informática.

Key words:

Data protection, privacy, digital rights, computing.